REMARKS

This Amendment responds to the Office Action dated March 27, 2003. A diligent effort has been made to respond to all of the objections and rejections contained in the Office Action and reconsideration is respectfully requested.

Claims 1-29, 42 and 43 remain pending in this application. Claims 30-41 have now been cancelled. The pending claims 1-29, 42 and 43 have not been amended.

A. Rejections over Wright, Adler and Moon

In paragraphs 3, 5-10, 13, and 14 of the Office Action, the pending claims were rejected over either Wright (US 6,084,969), Adler (US 6,157,630) or Moon (US 6,138,146), in a variety of 35 USC § 103 obviousness combinations. All of these rejections are moot, however, because none of these three patents are prior art to the present application as established by the enclosed Declaration of Prior Invention to Overcome Cited Patents Under 37 CFR § 1.131.

B. Claims 9, 13, 17, 23, 42 and 43

Claims 9, 13, 17, 23, 42 and 43 were ONLY rejected under various 35 USC § 103 combinations including Moon or Adler (*See*, Office Action, paragraphs 9, 10, 13 and 14). Because neither of these patents is prior art, however, the rejections must be withdrawn, and therefore there are no outstanding rejections of these claims. A notice of allowability is therefore respectfully requested with respect to claims 9, 13, 17, 23, 42 and 43.

C. Claims 1-8, 10-12, 14-16, 18-22 and 24-29

The remaining pending claims were rejected under various 35 USC § 103 combinations all relying on the disclosure of certain claimed subject matter from the Frith patent (US 5,943,426) (*See*, Office Action, paragraphs 11-20). These rejections must be withdrawn, however, because Frith clearly does not disclose this claimed subject matter as explained more fully below.

In paragraph 11, the Examiner rejected claims 1-8, 10, 16, 18, 22, 24 and 34 under 35 USC 103 as being unpatentable over Woltz (US 5,995,597) in view of Frith. In rejecting these claims the Examiner characterized Woltz as follows:

> ". . . Woltz discloses an electronic message redirection systems, as described previously. However, Woltz does not discuss the packaging, encryption, and/or compression of messages sent between the host and the mobile device." (Office Action at 15)

Having conceded that Woltz does not teach any of these three concepts from claim 1, the Examiner then argued that Frith discloses these concepts, stating that:

> "Frith discloses a system for redirecting messages received at a host (sending gateway) connected to a wired network, through a gateway (receiving gateway), to a wireless device (node) connected to a wireless network (col. 2, lines 38-61; Fig. 1), wherein the messages are packaged and encrypted at the host and remain packaged and encrypted until they reach the destination pager, and wherein the pager extracts the messages, thus establishing a secure electronic message redirection system (col. 5, line 64 - col. 6, line 7; col. 7, lines 5-17)."

There are several fundamental problems with this analysis. First, it ignores the actual claim language set forth in claim 1. And second, it completely mischaracterizes the limited teaching of the Frith patent.

Turning first to the claim language at issue, claim 1 sets forth a secure electronic message redirection system, comprising: (1) a host system having a redirector application, wherein the redirector application is configured to sense a trigger event at the host system and in response to the trigger event to continuously redirect electronic messages from the host system to a mobile data communication device; (2) a wired network coupled to the host system; (3) a wireless data network coupled to the mobile data communication device; (4) a wireless gateway coupled between the wired network and the wireless data network for transmitting messages between the wired network and the wireless network; and (5) ***a secure link formed between the host system and the mobile data communication device through the wireless gateway, the secure link formed using (A) an encryption module operating at the host system that encrypts the electronic messages prior to redirection to the mobile data communication device, and a corresponding decryption module operating at the mobile data communication device that decrypts the electronic messages that are received from the host system; wherein the host system further includes (B) a data compression module for compressing the electronic messages prior to redirecting the messages over the secure link through the wireless gateway, and the mobile data communication device includes a corresponding decompression module for decompressing the compressed electronic messages; wherein the host system includes (C) a packaging module for packaging the electronic messages into electronic envelopes prior to redirecting the messages over the secure link through the wireless gateway, and the mobile data communication device includes a corresponding unpackaging module for extracting the***

electronic messages from the electronic envelopes; and <u>wherein the electronic messages remain compressed, encrypted and packaged during redirection over the wired network, through the wireless gateway and over the wireless network to thereby establish a secure electronic message redirection system.</u> (<u>EMPHASIS ADDED</u>)

According to this claim, a secure electronic message redirection system is established including the host system where the redirector software is operating and the mobile communication device using three separate end-to-end techniques, (A) encryption; (B) compression; and (C) packaging into an electronic envelope. In order to accomplish this end-to-end secure link, corresponding encryption/decryption, compression/decompression; and packaging/unpackaging modules are located, respectively at the host system and the mobile device. The electronic messages are encrypted, compressed and packaged into electronic envelopes at the host system <u>AND REMAIN IN THAT STATE</u> until they are received at the mobile communication device. Importantly, the electronic messages remain in this encrypted, compressed and packaged form during the entire transmission path between the host system and the mobile communication device, including primarily through the wireless gateway that bridges the wired and wireless networks. In the prior art, such as Frith, the secure link was broken at the gateway.

The embodiment of Frith relied upon by the Examiner as showing the claim limitations set forth above simply does not provide the required teaching, but in fact <u>teaches away</u> from the claim language. In Frith there are two possibilities for routing messages: (i) the message is routed from a sending node (22) through a sending gateway (24) and directly to a destination node (20); or (ii) the message is routed from the sending node (22) through a sending gateway (24) and then to a receiving gateway (26) and then onto the destination node (20). It is only this

later embodiment that has any relation to claim 1, because in the first embodiment there is no redirection through a wireless gateway.

In the second embodiment, however, where messages are directed from the sending gateway (24) through the receiving gateway (26), the messages are not maintained in an encrypted form. See, for example, Figure 7, and associated description, showing the operation of the receiving gateway (24), in which the reduced (compressed) message is expanded at the receiving gateway and re-encrypted. ("Generally, when a signature of a reduced digitally signed message is verified, process 90 causes receiving gateway 26 to expand the reduced message into a restated message, and then the restated message is sent onward with a digital signature computed for receiving gateway 26 rather than sending node 22 or sending gateway 24.") See, also, Figures 3, 4 and 5, and associated description, in which it is clear that Frith is teaching the decryption and re-encryption of the messages at the gateways (24, 26). Thus, in Firth, just like in the other prior art systems, the security is not end-to-end, but is broken at the gateway.

In claim 1, the messages from the redirector remain encrypted, compressed and packaged into electronic envelopes **through the wireless gateway** and only become unpackaged, uncompressed and decrypted when they are received at the mobile communication device. By distinction, in Frith, the messages are decrypted and uncompressed at the receiving gateway, thus destroying the security of the system. It is precisely this end-to-end security problem through a gateway that claim 1 is directed to solving. Claim 1 is clearly distinguishable from Frith and a notice of allowability is therefore requested.

In addition, and despite the Examiner's contention to the contrary, there is absolutely no teaching whatsoever in Frith of the claim limitations of "***a packaging module for packaging the***

electronic messages into electronic envelopes prior to redirecting the messages over the secure link through the wireless gateway, and the mobile data communication device includes a corresponding unpackaging module for extracting the electronic messages from the electronic envelopes." The Examiner has, in fact, not pointed to any portion of Frith that would meet this claim language, and thus, for this additional reason, the rejection is improper and should be withdrawn.

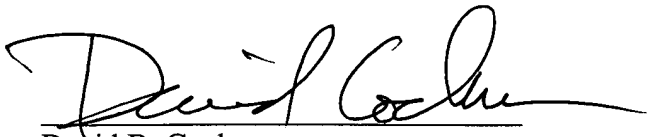
The remaining claims 2-8, 10-12, 14-16, 18-22 and 24-29 all include the same concept of maintaining an end-to-end secure link between the redirector and the mobile communication device through the wireless gateway, and thus are distinguishable from Frith for many of the same reasons discussed above. These claims are also, therefore, in condition for allowance.

D. Consideration of Information Disclosure Statements

Although the Examiner initialed several PTO-1449 submission made by the applicants in this case, there were two IDS forms that were not returned with the Office Action as being considered. A copy of the PTO-1449 for the first submission is attached hereto at Tab A, and was submitted by the applicants on February 12, 2001, along with the application. A copy of the second PTO-1449 is attached at Tab B, and this paper was submitted by the applicants on August 22, 2001. Applicants request that the Examiner consider the art in these two IDS forms and return the completed PTO-1449 forms along with the next communication in this application. If for some reason the forms were lost and do not appear in the file of this application, then the Examiner is asked to please contact the undersigned attorney for the applicants who will supply a replacement IDS.

Respectfully submitted,

JONES DAY



David B. Cochran
(Reg. No. 39,142)

Jones Day
North Point, 901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-7506